## REMARKS

This amendment is submitted with a petition for a one month extension of time and the requisite fee. Accordingly, the amendment is timely filed.

Claims 1-19 were pending and claims 1-19 were rejected. Claims 4, 6, 7, 11, 15, 16, and 19 have been amended, and claims 1-19 remain pending.

Claims 4, 6, 7, 11, 15, 16, and 19 have been amended to correct typographical errors. Applicants respectfully submit that these amendments are not narrowing and have not been made for reasons of patentability. Additionally, claim 11 has also been amended to recite "the encrypted download file encrypted using the unique user ID," and this amendment will be discussed in more detail below.

Claim 1-19 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Publication No. 2002/0012432 ("England"). With respect to claims 1-10 and 16-19, Applicants respectfully traverse the rejection and request withdrawal of the rejection. With respect to claims 11-15, Applicants respectfully request reconsideration in light of the amendment to claim 11 discussed below.

Claim 1

Claim 1 is directed to a digital information security system. The system comprises, *inter alia*, "a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal," and "a user management tool installed in a server, the user management tool being structured to receive the unique user key created by the user application tool, the user management tool being structured to store the received unique user key in the data storage unit, the user management tool being structured to compare the stored unique user key with a unique user key provided from the user application tool of a user currently being subjected to authentication."

The Office Action failed to establish that England discloses all the elements of claim 1. For example, the Office Action failed to establish that England discloses "a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal."

England describes a system for distributing encrypted digital content and allowing persons with rights to view the digital content to decrypt the content. The system

includes a content server, a license server, a black box server, and a user computing device. The content server downloads encrypted content to the user computing device in response to a request from the user. *See England* at par. 0077, Fig. 1. The user's computing device includes a rendering application that conditionally renders digital content and a digital rights management (DRM) system. *See id.* at par. 0120, Fig. 4. When a user attempts to render encrypted content downloaded from the content server, the rendering application invokes the DRM system. *See id.* at par. 0120. The DRM system checks whether the user has a license to render the downloaded content. If the user does not, the DRM system may download a license from the license server. *See id.* at par. 0011, Fig. 1. The license may include a decryption key to enable the user computing device to decrypt the digital content. *See id.* at par. 0012.

But the decryption key in the license is itself encrypted. *See id.* at par. 0017. A "black box" in the DRM system includes a public/private key pair. *See id.* at par. 0016. The license server uses the public key from the black box to encrypt the decryption key in the license, and the DRM system on the user computing device uses the private key from the black box to decrypt the decryption key in the license. *See id.* at par. 0017. The "black box" as well its public/private key pair is downloaded from the black box server to the user computing device. *See id.* at pars. 0016, 0178.

Although England describes a DRM system on a user computing device that utilizes a key in a license and keys in a black box, none of these keys are created by the DRM system. England describes the license server sending to the user computer the decryption key in a license. *See id.* at pars. 0011, 0012. But England does not appear to describe how the decryption key in the license is created. Additionally, England describes the black box server sending to the user computer the public/private key pair in the black box. *See id.* at pars. 0176, 0178. But England does not appear to describe how the keys in the black box are created. Thus, at least for this reason, the Office Action failed to establish that England discloses "a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal."

Additionally, England does not appear to teach anything about a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal. Although England describes the license server maintaining a list of "bad" users or computing devices

and not sending a license if the user or the user's computing device is on the list, England does not disclose that the decryption key in the license is created using unique system information of the user computing device. *See id.* at par. 0155. Similarly, although England describes the black box server creating a black box that will not allow rendering of content to proceed if the black box is not on the computing device for which it was created, England does not disclose that the public/private keys in the black box are created using unique system information of the user computing device. *See id.* at par. 0182. Thus, at least for this additional reason, the Office Action failed to establish that England discloses "a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal."

Claim 6

Claim 6 is directed to a digital information security method. The method comprises, "reading a first unique user key created using unique system information of a user terminal when a sever server is accessed by a user," "comparing the first unique user key with a second unique user key included in previously stored user information for the user, to authenticate whether the user is an authorized user," "encrypting a file uploaded by the authorized user using a preset encryption key, and storing the encrypted file as digital information," encrypting a decoding key for the corresponding digital information using the second unique user key included in the user information," and "downloading the encrypted decoding key along with the associated digital information in response to a digital information download request of the authorized user."

The Office Action failed to establish that England discloses all the elements of claim 6. For example, the Office Action failed to establish that England discloses "reading a first unique user key created using unique system information of a user terminal when a server is accessed by a user."

As discussed above with respect to claim 1, England does not disclose that the decryption key in the license is created using unique system information of the user computing device, does not disclose that the public/private keys in the black box are created using unique system information of the user computing device. *See id.* at par. 0182. Thus, the Office Action failed to establish that England discloses "reading a first unique user key

created using unique system information of a user terminal when a server is accessed by a user."

Claim 10

Claim 10 is directed to a digital information security method. The method comprises, *inter alia*, "creating a unique user key at a user terminal using unique system information of the user terminal."

The Office Action failed to establish that England discloses all the elements of claim 10. For example, the Office Action failed to establish that England discloses "creating a unique user key at a user terminal using unique system information of the user terminal" at least for reasons similar to those discussed above with respect to claim 1.

Claim 11

Claim 11 is directed to a digital information security system. The system comprises, *inter alia*, "a key management service module installed in a user system, the key management service module being structured to encrypt user information including a unique user ID created based on system information of a corresponding user from a user application tool installed in a system of the user, and storing the encrypted user information," and "a document distribution service module structured to create an encrypted download file including information on an output rule of the file in a predetermined user environment when downloading the file to the user." Additionally, claim 11 has been amended to recite "the encrypted download file encrypted using the unique user ID."

England does not disclose all the elements of claim 11. For example, England does not teach anything about a unique user ID created based on system information of a user and then encrypting a download file using the unique user ID. At least for this reason, claim 11 is allowable.

Claim 16

Claim 16 is directed to a digital information security method related to a file that has been uploaded by a user. The method comprises, *inter alia*, "transmitting by the web server information on the uploaded file to the document management service gateway," "reading by the document management service gateway the uploaded file by accessing a

position where the file is actually uploaded from the server, using the information on the uploaded file," "creating a document key for the read file in a predetermined decoding method, and storing the created document key along with the corresponding file information," "encrypting the file using the created document key," "storing the encrypted file in a predetermined folder," and "informing the web server that processing of the uploaded file is completed."

England describes an authoring tool and a content server. *See England* at Fig. 1. The authoring tool encrypts content and the content server distributes the encrypted content. *See id.* at par. 0048, 0076. But England does not disclose the combination of elements recited in claim 16. For example, England does not disclose "reading by the document management service gateway the uploaded file by accessing a position where the file is actually uploaded from the server, using the information on the uploaded file," "storing the encrypted file in a predetermined folder," and "informing the web server that processing of the uploaded file is completed." Accordingly, the Office Action failed to establish that England discloses all the elements of claim 16.

Other Claims

Claims 2-5 depend from claim 1. It is respectfully submitted that claims 2-5 are allowable for the same reasons as claim 1, as well as for additional reasons.

Claims 7-9 depend from claim 6. Applicants respectfully submit that claims 7-9 are allowable for the same reasons as claim 6, as well as for additional reasons.

Claims 12-15 depend from claim 11. It is respectfully submitted that claims 12-15 are allowable for the same reasons as claim 11, as well as for additional reasons.

Claims 17-19 depend from claim 16. Applicants respectfully submit that claims 17-19 are allowable for the same reasons as claim 16, as well as for additional reasons.

## Conclusion

In view of the above, Applicants believes that claims 1-19 are allowable and that the pending application is in condition for allowance.

Dated: June 9, 2005

Respectfully submitted,

By _____
Gregory E. Stanton
Registration No.: 45,127
MARSHALL, GERSTEIN & BORUN LLP
233 S. Wacker Drive, Suite 6300
Sears Tower
Chicago, Illinois 60606-6357
(312) 474-6300
Attorney for Applicants